National Aeronautics and
Space Administration

Goddard Space Flight Center
Greenbelt, MD 20771

Reply to Attn of: 297

2002

TO: Summer Program Participants

FROM: 297/Center Information Technology Security Manager

SUBJECT: Information Technology Security (ITS)

During you brief stay here at Goddard Space Flight Center (GSFC), you will probably use one or more of the extensive computing facilities that are located at Greenbelt, Wallops Flight Facility (WFF), Independent Verification & Validation Facility (IVV), and the Goddard Institute for Space Studies (GISS). We have literally thousands of computers from laptop computers to supercomputers. Most of our computers are connected to the Internet, allowing us to share automated information with fellow worldwide computer users. While this "open" environment facilitates our primary missions of earth and space research, it creates some significant vulnerabilities in terms of securing our systems and networks. The success of NASA's most important missions depends on the accuracy, reliability and availability of automated information, making security of our information technology (IT) systems and networks a principal concern. You may have worked or studied in similar "open" computing environments, but probably have not encountered the level of security which the Center currently requires. To assist you, I have listed some things you can do to avoid causing a security violation. When you finish reading this memorandum, please sign the enclosed form and return it as indicated. If you have any questions, ask your supervisor for clarification.

- **Complete IT Security training -- "Basic IT Security for 2002" available on the NASA Site for ON-Line Learning and Resources (SOLAR) at https://solar.msfc.nasa.gov:443/solar/delivery/public/html/newindex.htm or view the CD entitled "Introduction to Information Technology Security for New Employees".**

Use GSFC computers and networks to do authorized work only. Unauthorized access to and/or use of a government computer system or network is a violation of law and punishable under provisions of 18 USC 1029, 18 USC 1030, and other applicable statutes. Not only is it against the law, but also it reduces the availability of computer resources for legitimate work.

- **Passwords -- select good ones and protect them.** A good password contains at least eight characters (one each from three of these set of characters - uppercase letters, lowercase letters, numbers, special characters). Your password should not be the same as your user ID. Protect your password by not sharing it with anyone, writing it down, or storing it electronically in your computer. Use of a password is a primary safeguard against "hackers." In a networked environment such as ours, their importance cannot be overstated. It is your responsibility to secure your password. Change it if you suspect it has been compromised, and do not access GSFC systems and networks using someone else's password.

- **Imported software -- do not install it without prior approval.** There have been instances in which software obtained from friends, bulletin boards, and other private sources has contained viruses or malicious code that either destroyed data or caused other undesirable effects. In response to this problem, NASA has published the following policy.

> "It is NASA policy to use imported software, including but not limited to: freeware, public domain software, shareware, and licensed software, only after the software has been reasonably determined to be safe for use in its intended environment. It is also NASA policy to require registration and/or licensing of software as requested by the author or vendor."

To insure you are complying with this policy, obtain the approval of your system administrator and/or supervisor before installing any software on a GSFC computer system or network, to include personal computers.

- **Unauthorized software -- do not make, acquire, or use it.** Unauthorized duplication of licensed or copyrighted software is a **Federal crime.** Retain purchase records, original disks, documentation and/or licensing agreements to prove your software is legal. You have the right to make a back-up copy of software if the vendor provided none. To stay out of trouble, follow the one software package/one computer rule.

- **Connection to a Center network -- do not connect your non-government computer to a Center network without obtaining permission.** All computers must undergo a vulnerability scan prior to connecting to a Center network. Your supervisor must approve your connecting to a Center network.

- **Electronic Mail** -- Do not open unsolicited e-mail attachments without verifying their source.

- **Back-ups -- you will be sorry if you do not have them**. Your system will crash, you will accidentally delete a file you need, and you are likely to encounter a virus, worm, etc. It's Murphy's Law at its finest! While backing-up your work will not prevent any of these things from happening, it will certainly help ease the pain. As a rule, you should back-up your work twice a month, more frequently on files, which you change often. Remember that you will probably have to reconstruct everything since your last back up.

- **Information -- protects it.** The different NASA information categories --Mission (MSN), Business and Restricted Technology (BRT), Scientific, Engineering and Research (SER), Administrative (ADM) and Public (PUB require different levels of protection. Before you enter information into an IT system, insure that the system provides at least the level of protection required by the information category you plan to enter. If you need help in making this determination consult your supervisor.

- **Logoff -- do it any time you leave your workstation unattended.** Studies consistently show that people who work within the organization commit the majority of computer mischief. When you leave your computer logged onto a system or network, you provide an excellent opportunity for unauthorized "experimentation." Further, when it's all over, the audit trail will lead to you!

- **Security Violations -- if you suspect one, report it.** Be alert for unexplainable changes in your computing environment. If you think someone, or something, has tampered with your system, immediately inform your supervisor.

As a former NASA Administrator stated --

> "Assuring the security and integrity of NASA's computer systems and electronic information is the responsibility of <u>all</u> our employees… I cannot over-emphasize the importance that I attach to protecting the reliability and accuracy of our information resources."

The bottom line is that we are concerned about the security of our information technology resources as we think you should be too. Remember being the source of a security violation or embarrassment to NASA is not a career-enhancing experience!

Henry J. Middleton

Henry J. Middleton
Enclosure